UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN

Cheryl Drugich, et al., Plaintiffs, v. McLaren Health Care Corporation, Defendant.	Case No. 2:23-cv-12520-MFL-CI Hon. Matthew F. Leitman **CLASS ACTION** **JURY TRIAL DEMANDED**

FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

TABLE OF CONTENTS

Plaintiffs Cheryl Drugich, Janise Norwood, Melissa Porter, Jamie McSkulin, Tamyra Ejuan Wells, Ashley Beasley, Kyle Turri, and Trista Wynn Stebbins (collectively, "Plaintiffs") bring this First Amended Consolidated Class Action Complaint against McLaren Health Care Corporation ("McLaren" or "Defendant"), individually and on behalf of all others similarly situated, and allege as follows:

NATURE OF THE ACTION

1. Healthcare providers that are entrusted with patients' sensitive personally identifying information ("PII") or protected health information ("PHI") (together, "Private Information") owe a duty of care to those individuals to protect that information. This duty arises because it is foreseeable that the exposure of PII and PHI to unauthorized persons – especially hackers and other cybercriminals with nefarious intentions – will result in harm to the affected individuals.

2. Because of the highly sensitive nature of the data collected and maintained during the course of providing patient care, healthcare providers like McLaren are leading targets for cyber-attacks. The rapid growth of electronic medical recordkeeping, online medical services, and mobile medical apps has created new pressure points for criminals to exploit.

3. States have enacted strict laws requiring entities that collect and maintain patient information to ensure they take the utmost care to protect the privacy of the data they hold. In 2004, for example, Michigan enacted the Identify

Theft Protection Act (MCL 445.61, *et seq.*), requiring entities that have experienced a data breach to promptly notify those affected of the nature and quality of the breach. And when Michigan amended the Nonprofit Health Care Corporation Reform Act (MCL 500.1400, *et seq*.) in 2006, it included a requirement that all health care corporations take care to secure records that include PII, and created a private right of action for a failure to safeguard that data.

4. McClaren itself recognizes the importance of data security, telling patients that "[w]e protect the privacy of your health information" and "we seek to use reasonable measures to protect Personally Identifiable Information[.]"[1]

5. Despite this professed recognition, McLaren failed to take appropriate measures to safeguard the sensitive data entrusted to it from the foreseeable event of a data breach. And it has now been the subject of two back-to-back breaches.

6. According to McLaren, there initially "was unauthorized access to McLaren's network between July 28, 2023 and August 23, 2023"[2] (herein after the "2023 Data Breach"). For nearly a month, unauthorized hackers were able to access the McLaren computer network and extract 3.2 TB of data without being detected.

---

[1] *Web Privacy Policy*, McLAREN, https://www.mclaren.org/main/web-privacy-policy (last accessed Oct. 17, 2024).

[2] *Data Breach Notifications*, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/40c59f93-d7fd-4133-8148-a05a244b96b7.shtml at **McLaren - Notice of Data Event - ME.pdf** (last accessed Oct. 17, 2024).

7. McLaren claims to have first become aware of "suspicious activity related to its computer systems" on August 22, 2023. But it was not until October 20, 2023 that it began to provide "substitute . . . website and media notice," and then not until November 9, 2023 that it began mailing notification of the 2023 Data Breach directly to its current and former patients and other affiliated persons.[3]

8. According to McLaren's notice concerning the 2023 Data Breach, it determined that "the unauthorized actor had the ability to acquire certain information stored on the network during the period of access" and that "information pertaining to certain individuals may have been included in the potentially accessed files" – the compromised data included names, Social Security numbers, health insurance information, birthdates, and medical information (including diagnosis, physician information, "prescription/ medication information," and "diagnostic and treatment information").[4]

9. McLaren's form letters to its current and former patients and other affiliated persons did not identify who the "unauthorized actor" was, address whether a ransomware demand was made and/or paid, or indicate if any of the compromised patient data had been placed on the dark web (the illicit marketplace where thieves and criminals trade stolen PII and PHI in bulk).

[3] *Id.*
[4] *Id.*

10. A report issued on October 4, 2023 revealed that the notorious hacking collective BlackCat/AlphV had posted "that it stole 6 terabytes of McLaren's data" and further boasted about this being "one of the biggest leaks of all time" – the group is claimed to have told McLaren "[o]ur backdoor is still running on your network."[5]

11. On October 6, 2023, Michigan Attorney General Dana Nessel issued a press release which indicated that that "[c]ybercriminal gang ALPHV (or BlackCat) has claimed responsibility for the theft of the sensitive personal health information (PHI) of 2.5 million McLaren patients."[6] The press release stated that this cybercriminal group had also been linked to the recent attack at MGM Resorts, and had posted a message on the dark web the previous week claiming that "the McLaren data was on the dark web and would be released in a few days unless a ransomware payment was received."[7]

12. Attorney General Nessel stated in this press release that "[o]rganizations that handle our most personal data have a responsibility to

---

[5] Jordan Shamus, Kristen, *McLaren ransomware attack may have leaked patient data to dark web* (Oct. 4, 2024) https://www.freep.com/story/news/health/2023/10/04/mclaren-michigan-ransomware-attack-blackcat-alphv-dark-web-cybersecurity-breach-health/71056856007/.

[6] *AG Nessel Notifies Michigan Residents of McLaren Ransomware Attack Threatening to Expose Patient Data*, MICHIGAN DEPT. OF ATTY. GEN. (Oct. 6, 2023) https://www.michigan.gov/ag/news/press-releases/2023/10/06/ag-nessel-notifies-michigan-residents-of-mclaren-ransomware-attack.

[7] *Id.*

implement safety measures that can withstand cyber-attacks and ensure that a patient's private health information remains private" – and she also indicated "[t]ime is of the essence when a breach occurs to ensure affected individuals can take the necessary steps to protect their identities."[8]

13. Despite having experienced the 2023 Data Breach less than a year ago, McLaren failed to make the necessary security upgrades to ensure the protection of its systems and of the Private Information of Plaintiffs and the Class going forward.

14. Accordingly, due to these failures, McLaren experienced *another* data security incident nearly a year later. Pursuant to a statement issued by McLaren on August 7, 2024, "McLaren Health Care can now confirm the disruption to our information technology and phone systems that was reported yesterday [August 6, 2024] was the result of a criminal cyber attack."[9]

15. Upon information and belief, McLaren first became aware of this external breach even earlier (hereinafter known as "2024 Data Breach"), on August 5, 2024, through a ransomware demand sent through and among its information technology systems.[10]

---

[8] *Id.*

[9] *See* https://www.chiefhealthcareexecutive.com/view/michigan-hospital-system-suffers-cyberattack-again (last accessed Oct. 17, 2024).

[10] Ellis, Mike, *Ransomware attack confirmed by McLaren; health system says impact ongoing through August*, LANSING STATE JOURNAL (Aug. 17, 2024), https://www.lansingstatejournal.com/story/news/local/2024/08/17/ransomware-attack-mclaren-health-care-patients-services-appointments/74840781007/.

16. As a result of McLaren's inadequate security measures, and in breach of its legal duties and obligations, both the 2023 Data Breach and the 2024 Data Breach (collectively, "Data Breaches") occurred, putting the Private Information of Plaintiffs and the Class at risk for the foreseeable future.

17. As a result of McLaren's inadequate security measures, and in breach of its legal duties and obligations, the Data Breaches occurred, and several Plaintiffs, as representatives of the enormous class of individuals here, have experienced suspicious and fraudulent activity as a result thereof.

18. Plaintiffs' counsel have confirmed that, at the very least, the PII and PHI compromised in the 2023 Data Breach was actively offered for sale to third-parties on the dark web. In the course of attempting to extract a ransomware payment, BlackCat indicated that it still had access to McLaren's network over a month after McLaren had first detected it. Plaintiffs do not know whether McLaren actually paid the ransomware demand and, if so, what if anything it received in exchange.

19. As a result of the Data Breaches, Plaintiffs and at least 2.5 million class members suffered concrete injuries in fact including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; (v) loss of benefit of the

bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

20. Plaintiffs' claims are brought as a class action, pursuant to Federal Rule of Civil Procedure 23, on behalf of themselves and all other similarly situated persons. Plaintiffs seek relief in this action individually and on behalf of a similarly situated class of individuals for negligence, breach of implied contract, breach of express contract, violations of the Michigan Consumer Protection Act, violations of the Michigan Data Breach Notification Statute, violations of the Nonprofit Health Care Corporation Reform Act and, alternatively, unjust enrichment. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

21. Plaintiffs seek remedies including, but not limited to, compensatory, nominal, punitive and statutory damages, as well as injunctive relief mandating improvements to McLaren's data security systems and the provision of appropriate identity theft and monitoring services.

PARTIES

22. Plaintiff Cheryl Drugich is a natural person and citizen of Michigan, where she intends to remain.

23. Plaintiff Janise Norwood is a natural person and citizen of Michigan, where she intends to remain.

24. Plaintiff Melissa Porter is a natural person and citizen of Michigan, where she intends to remain.

25. Plaintiff Jamie K. McSkulin is a natural person and citizen of Michigan, where she intends to remain.

26. Plaintiff Tamyra Ejuan Wells is a natural person and citizen of Michigan, where she intends to remain.

27. Plaintiff Ashley Beasley is a natural person and citizen of Michigan, where she intends to remain.

28. Plaintiff Kyle Turri is a natural person and citizen of Michigan, where he intends to remain.

29. Plaintiff Trista Wynn Stebbins is a natural person and citizen of Michigan, where she intends to remain.

30. Defendant McLaren Health Care Corporation is a non-profit corporation organized under the state laws of Michigan. Its principal place of business is in Grand Blanc, Michigan.

JURISDICTION AND VENUE

31. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

32. This Court has personal jurisdiction over McLaren because its principal place of business is in this District, it regularly conducts business in Michigan, and the acts and omissions giving rise to Plaintiffs' claims occurred in and emanated from this District.

33. Venue is proper under 18 U.S.C § 1391(b)(1) because McLaren's principal place of business is in this District.

FACTUAL ALLEGATIONS

Background

34. McLaren "is a $6.6 billion, fully integrated health care delivery system" that "includes 13 hospitals in Michigan, ambulatory surgery centers, imaging centers, a 490-member employed primary and specialty care physician network, commercial and Medicaid HMOs covering more than 732,838 lives in Michigan and Indiana[.]"[11]

[11] *McLaren Health Care - Doing What's Best*, MCLAREN,

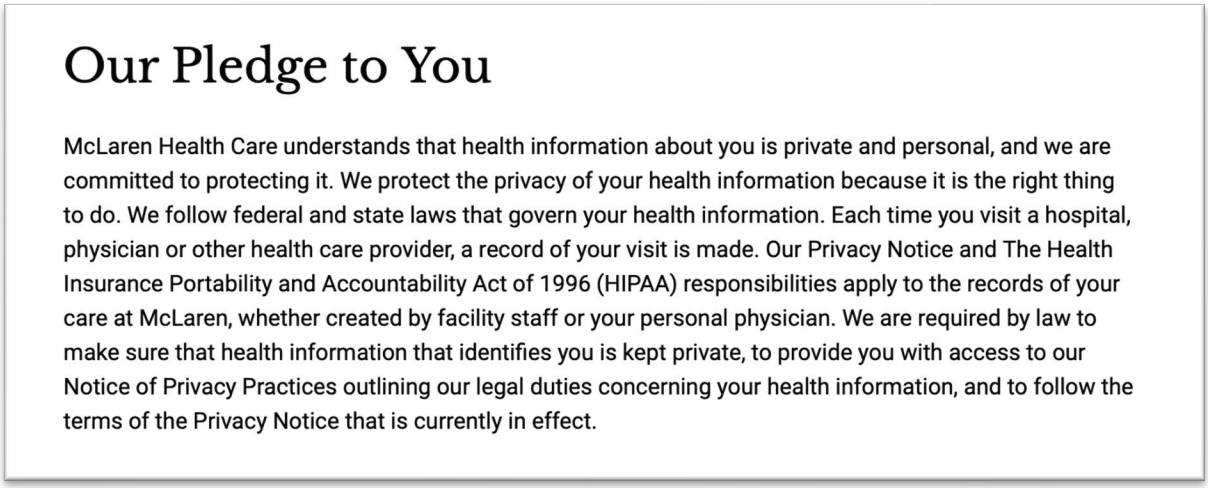
35. Members of the proposed class here, which includes Plaintiffs, are current and former patients of McLaren and other affiliated persons whose PII and/or PHI was compromised as a result of the Data Breaches ("Class Members").

36. McLaren creates, collects, and receives treatment records, lab testing data, demographic information, and payment information from its patients and other affiliated persons. Patients entrusted McLaren with this information, which, by its nature, is confidential and highly sensitive and may include their medical histories, current conditions, medications, Social Security numbers, credit card numbers, and other sensitive PII and PHI.

37. Because of the highly sensitive nature of the information it collects, McLaren makes many promises regarding the protection of patient data. Its Compliance Program and Resources page, for example, contains a "pledge" to protect the privacy of patient's data:

---

https://www.mclaren.org/main/about-mclaren-health-care (last accessed Oct. 17, 2024).



Our Pledge to You

McLaren Health Care understands that health information about you is private and personal, and we are committed to protecting it. We protect the privacy of your health information because it is the right thing to do. We follow federal and state laws that govern your health information. Each time you visit a hospital, physician or other health care provider, a record of your visit is made. Our Privacy Notice and The Health Insurance Portability and Accountability Act of 1996 (HIPAA) responsibilities apply to the records of your care at McLaren, whether created by facility staff or your personal physician. We are required by law to make sure that health information that identifies you is kept private, to provide you with access to our Notice of Privacy Practices outlining our legal duties concerning your health information, and to follow the terms of the Privacy Notice that is currently in effect.

McLaren's 2020 Standards of Conduct claims:

> A COMMITMENT TO CONFIDENTIALITY AND ELECTRONIC SECURITY [. . .]
>
> It is the responsibility of every employee, physician, volunteer, and contractor or vendor to adhere to regulations, policies/procedures, and patient rights for privacy . . .

38. McLaren's June 2022 Notice of Privacy Practices claims:

> OUR PLEDGE TO YOU
>
> We understand that health information about you is private and personal, and we are committed to protecting it. [. . .]
>
> Notification of a Breach: If our actions result in a breach of your unsecured health information we will notify you of that breach.

39. Indeed, the Privacy Policy posted on Defendant's website provides that: "we seek to use reasonable measures to protect Personally Identifiable Information[.]"[12]

[12] *Web Privacy Policy*, *supra*, n.1.

40. Plaintiffs and Class Members, as former and current patients of McLaren and other affiliated persons, relied on these promises and on this sophisticated business entity to keep their sensitive Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Patients, in general, demand security to safeguard their Private Information, especially when PHI and other sensitive PII is involved.

41. McLaren did not keep its pledge to maintain patient privacy. Based on the nature of the Data Breaches and the statements of the unauthorized users who gained access to the McLaren networks on at least two separate occasions, it is apparent that McLaren's system failed to employ reasonable and appropriate security measures with regard to any or all of the following: storing data in secure, offline locations; encrypting private records and data; using up-to-date software equipped with standard security patches; using anti-virus applications that block malicious code from external sources; and implementing policies requiring all workers with system access to use https protocols when using online tools.

42. Defendant's failure to adequately employ these and other industry-standard security measures needlessly exposed and continues to expose patients and other affiliated persons whose data was stored with Defendant to the risk of data theft.

The Two Data Breaches at McLaren

43. On or around August 22, 2023, McLaren "detected 'suspicious activity' on its computer network, immediately launched an investigation into the source of the disruption, and retained outside global cybersecurity specialists to assist[.]"[13]

44. As a result of its investigation, Defendant "determined that [McLaren] did experience a ransomware event."[14]

45. On or about September 29, 2023, ALPHV ransomware cybercrime collective, also known as BlackCat, took credit for the 2023 ransomware attack and further claimed "to have stolen 6 terabytes of data on 2.5 million patients[.]"[15]

46. BlackCat was already a threat actor known to McLaren at the time the 2023 Data Breach occurred and McLaren had been warned of its methods and strategies. In January 2023, the U.S. Department of Health and Human Services' Office of Information Security and Health Sector Cybersecurity Coordination Center issued a joint statement and brief warning entities in the healthcare sector, including McLaren, that ransomware attacks from BlackCat posed a specific threat to the industry.[16] The warning specified the operating systems that were especially

[13] McGee, Marianne Kolbasuk, *Group Claims It Stole 2.5 Million Patients' Data in Attack*, DATA BREACH TODAY, (Oct. 3, 2023) https://www.databreachtoday.com/group-claims-stole-25-million-patients-data-in-attack-a-23212.
[14] *Id.*
[15] *Id.*
[16] *Royal & BlackCat Ransomware: The Threat to the Health Sector*, (Jan. 12,

vulnerable to attack, entry points it was likely to use to access data, the technical operations it employed to attack targets, the tools it used to access and exfiltrate data, and a series of mitigation and defense strategies healthcare providers should use to defend their patients' PHI and PII.[17]

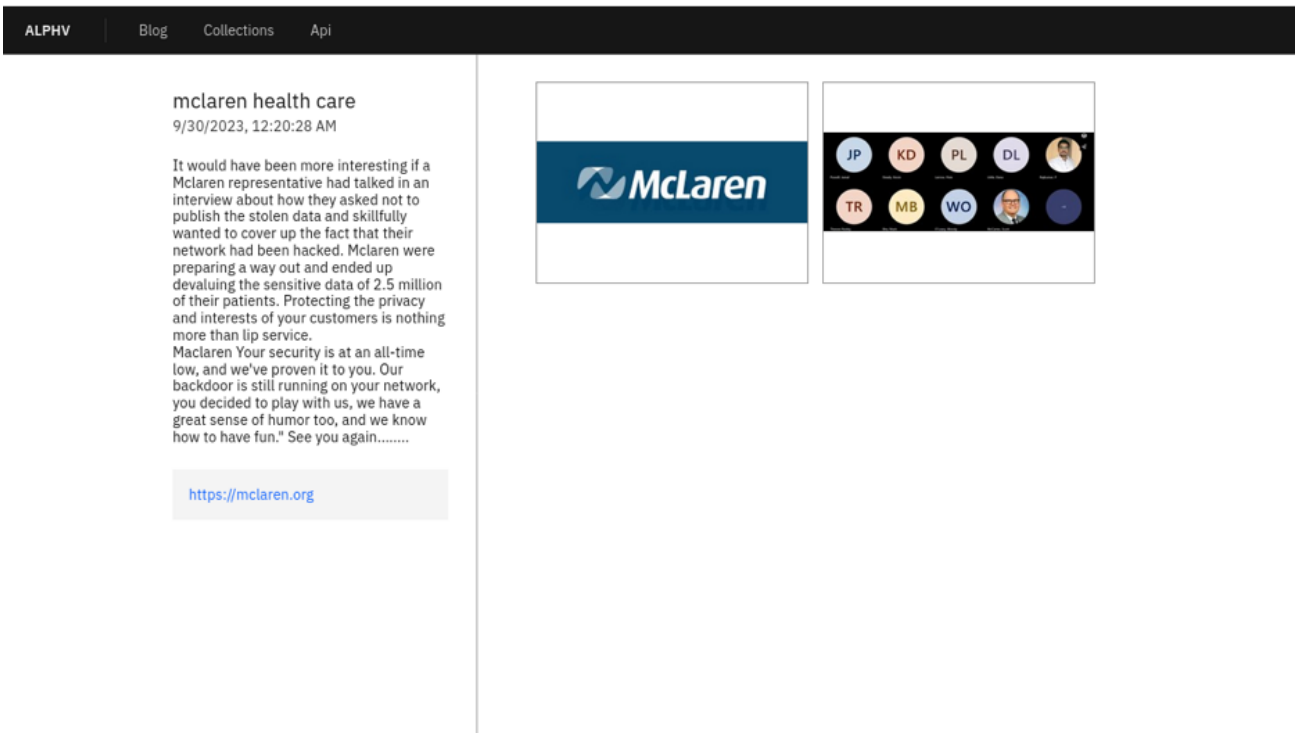
47. Based on the nature of the 2023 Data Breach and the statements of the unauthorized users who gained access to the McLaren networks, Plaintiffs allege, on information and belief, that Defendant failed or refused to heed the warnings from the January 2023 briefing, continued to use vulnerable systems, and neglected to employ the mitigation and defense strategies it was urged to use, which resulted in the 2023 Data Breach.

48. Upon information and belief, Blackcat attempted to negotiate a ransom with Defendant.

49. When BlackCat announced the Breach publicly on its TOR leak site on September 30, 2023, it indicated that it still had access to the McLaren network through backdoors that remained open.

2023) https://www.hhs.gov/sites/default/files/royal-blackcat-ransomware-tlpclear.pdf.

[17] *Id.*



50. The message published by BlackCat on its leak site reads: "It would have been more interesting if a Mclaren [sic] representative had talked in an interview about how they asked not to publish the stolen data and skillfully wanted to cover up the fact that their network had been hacked. Mclaren were preparing [sic] a way out and ended up devaluing the sensitive data of 2.5 million of their patients. Protecting the privacy and interests of your customers is nothing more than lip service. Mclaren [sic] Your security is at an all-time low, and we've provien [sic] it to you. Our backdoor is still running on your network, you decided to play with us, we have a great sense of humor too, and we know how to have fun.' See you again[.]"

51. Follow up posts on the BlackCat TOR leak site provide evidence of the data exfiltrated from McLaren including database scheme (including table names),

screen shots of table rows with fields and data, and directory structures.

52. BlackCat then posted on its TOR leak site on October 4, 2023 that it had confirmed to McLaren the data in its possession and would start auctioning data within 72 hours, with time remaining to salvage McLaren's data security reputation, inferring that there was still time to pay an unpaid ransom. Notably, McLaren did not disclose this fact in its Notice Letter, nor did it alert Plaintiffs and Class Members that BlackCat had acquired over 6 terabytes of McLaren's data.

53. Then, on October 19, 2023, a threat actor, "IAmNietzche," started selling McLaren data, from the 2023 Data Breach, on the forum_XSS for $50,000. On the post, IAmNietzche provided screenshots of the McLaren data, which showed details such as patient information, insurance details, lab test data, doctor information, visit information, and medication management system data. The total size of the database was approximately 3.2TB.

54. The data remained for sale on the dark web through at least the following month. By November 7, 2023, IAmNietzche was still selling the data at the reduced price of $15,000.

55. While it is not known with certainty how BlackCat gained access to McLaren's network, it is clear that there were thousands of McLaren credentials readily available on the dark web. The availability of those credentials suggests a canary in the coal mine warning of inadequate security practices in the overall

culture at McLaren.

56. In the period between July 28, 2023 and August 22, 2023, BlackCat and/or its affiliate, had removed 3.2 TB of data from the McLaren network undetected. This suggests there is a lack of security controls and policies in place that should have detected and prevented this type of incident from occurring.

57. Despite having experienced the 2023 Data Breach less than a year prior, McLaren failed to make the necessary security upgrades to ensure the protection of its systems and of the Private Information of Plaintiffs and the Class going forward, and, accordingly, due to these failures, McLaren experienced *another* data security incident less than a year later.

58. Pursuant to a statement issued by McLaren on August 7, 2024 regarding the 2024 Data Breach, "McLaren Health Care can now confirm the disruption to our information technology and phone systems that was reported yesterday [August 6, 2024] was the result of a criminal cyber attack."[18]

59. Upon information and belief, McLaren first became aware of this external breach even earlier, on August 5, 2024, through a ransomware demand sent through and among its information technology systems.[19]

[18] *See* https://www.chiefhealthcareexecutive.com/view/michigan-hospital-system-suffers-cyberattack-again (last accessed Oct. 17, 2024).
[19] *Ellis*, *supra*, n.10.

60. According to McLaren's August 7, 2024 statement, its "information technology team continues to work with external cyber security experts to analyze the nature of the attack and mitigate the impacts of the threat actors."[20]

61. Upon information and belief, the unauthorized users who gained access to McLaren's networks advised McLaren that they had stolen Private Information and would release the data unless a ransom was paid through the dark web.

62. Based on the nature of the 2024 Data Breach and the statements of the unauthorized users who gained access to the McLaren networks, Plaintiffs allege, on information and belief, that Defendant failed or refused to heed the warnings from McLaren's own 2023 Data Breach, continued to use vulnerable systems, and neglected to employ the mitigation and defense strategies it was urged to use, which resulted in the 2024 Data Breach.

63. Especially given the proximity of the most recent data breach at McLaren, this suggests that there is a lack of security controls and policies in place that should have detected and prevented this type of incident from occurring.

64. As evidenced by the 2024 Data Breach's occurrence, upon information and belief, the Private Information contained in Defendant's network was not encrypted.

65. As a result of McLaren's inadequate security measures, and in

[20] *Id.*

breach of its legal duties and obligations, the Data Breaches occurred, putting the Private Information of Plaintiffs and the Class at risk for the foreseeable future.

The Nature of Ransomware Cyberattacks

66. A ransomware attack is a type of cyberattack that is frequently used to target companies due to the sensitive patient data they maintain.[21] In a ransomware attack, the attackers use software to encrypt data on a compromised network, rendering it unusable and demanding payment to restore control over the network.[22]

67. Ransomware attackers do not just hold networks hostage: "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[23] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence […] the initial assumption should be that data may have been exfiltrated."

68. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and

---

[21] Palmer, Danny, *Ransomware warning: Now attacks are stealing data as well as encrypting it*, ZDNET, (July 14, 2020), https://www.zdnet.com/article/ransomware-warning-now-attacks-are-stealing-data-as-well-as-encrypting-it/.

[22] *Ransomware: The Data Exfiltration and Double Extortion Trends*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends (last accessed Oct. 17, 2024).

[23] *The chance of data being stolen in a ransomware attack is greater than one in ten*, EMSISOFT, (July 13, 2020), https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/.

exfiltrates the data contained within.[24] In 2020, over 50% of ransomware attackers exfiltrated data from a network before encrypting it.[25] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] it will be traded to other threat actors, sold, or held for a second/future extortion attempt" – and even where companies pay for the return of data, attackers often leak or sell the data regardless because there is no way to verify that copies of the data are destroyed.[26]

69. Ransomware attacks are particularly harmful for patients and healthcare providers alike, as they cause operational disruptions that result in lengthier patient stays, delayed procedures or test results, increased complications from surgery, and even increased mortality rates.[27] In 2021, 44% of healthcare providers who experienced a ransomware attack saw their operations disrupted for up to a week and 25% experienced disrupted services for up to a month.[28]

---

[24] *Ransomware Demands continue to rise as Data Exfiltration becomes common, and Maze subdues*, COVEWARE, (Nov. 4, 2020), https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report.
[25] *Ransomware FAQs*, https://www.cisa.gov/stopransomware/ ransomware-faqs (last accessed Oct. 17, 2024).
[26] *Id.*
[27] Jerich, Kat, *Ponemon study finds link between ransomware, increased mortality rate*, HEALTHCARE IT NEWS, (Sept. 22, 2021) https://www.healthcareitnews.com/news/ponemon-study-finds-link-between-ransomware-increased-mortality-rate.
[28] SOPHOS, *The State of Ransomware in Healthcare 2022*, (May 2020), https://assets.sophos.com/X24WTUEQ/at/4wxp262kpf84t3bxf32wrctm/sophos-state-of-ransomware-healthcare-2022-wp.pdf.

70. Upon information and belief, the cyberattacks here were targeted at Defendant due to its status as a healthcare entity that collects, creates, and maintains Private Information on its computer networks and/or systems.

71. Plaintiffs' and Class Members' Private Information was compromised and acquired in the Data Breaches.

72. The files containing Plaintiffs' and Class Members' Private Information that were targeted and stolen from Defendant included Plaintiffs' and Class Members' PII and/or PHI.

73. Because of this targeted cyberattack, data thieves were able to gain access to and obtain data from Defendant that included the Private Information of Plaintiffs and Class Members.

74. As evidenced by the Data Breaches' occurrence, the Private Information contained in Defendant's network was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

75. Defendant had obligations created by the FTC Act, HIPAA, contract, state and federal law, common law, and industry standards to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

Data Breaches Are Foreseeable and Preventable

76. McLaren did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiffs and Class Members, such as encrypting the information or deleting it when it is no longer needed, causing the exposure of Private Information.

77. McLaren could have prevented these Data Breaches by, among other things, properly encrypting or otherwise protecting its equipment and computer files containing Private Information.

78. To prevent and detect cyber-attacks and/or ransomware attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, patients and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/ LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[29]

79. To prevent and detect cyber-attacks or ransomware attacks, Defendant

[29] *Ransomware FAQs*, *supra*, n.25.

could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

> **Secure internet-facing assets**
> - Apply latest security updates
> - Use threat and vulnerability management
> - Perform regular audit; remove privileged credentials;
>
> **Thoroughly investigate and remediate alerts**
> - Prioritize and treat commodity malware infections as potential full compromise;
>
> **Include IT Pros in security discussions**
> - Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;
>
> **Build credential hygiene**
> - Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;
>
> **Apply principle of least-privilege**
> - Monitor for adversarial activities
> - Hunt for brute force attempts
> - Monitor for cleanup of Event Logs
> - Analyze logon events;
>
> **Harden infrastructure**
> - Use Windows Defender Firewall
> - Enable tamper protection
> - Enable cloud-delivered protection
> - Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[30]

[30] *See* Microsoft Threat Intelligence, *Human-operated ransomware attacks: A preventable disaster* (Mar 5, 2020), MICROSOFT, https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

80. Given that McLaren was storing the PII and PHI of its current and former patients and other affiliated persons, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

81. The occurrence of the back-to-back Data Breaches indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breaches and the exposure of the Private Information of, upon information and belief, over 2.5 million patients, including that of Plaintiffs and Class Members.[31]

McLaren Acquires, Collects, and Stores Patients' Private Information

82. In the regular course of its business operations, McLaren acquires, collects, and stores a massive amount of PII and PHI on its patients, former patients and other affiliated persons.

83. As a condition of obtaining medical services at McLaren, Defendant requires that patients entrust it with highly sensitive Private Information.

84. By obtaining, collecting, and using Plaintiffs' and Class Members' Private Information, McLaren assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

85. Plaintiffs and Class Members have taken reasonable steps to maintain

[31] *McGee*, *supra*, n.13.

the confidentiality of their Private Information and would not have entrusted it to Defendant absent a promise to safeguard that information.

86. Plaintiffs and Class Members relied on McLaren to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and make only authorized disclosures of this information.

McLaren Knew That Cybercriminals Target Private Information

87. McLaren's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities that collect and store Private Information, like Defendant, preceding the date of the Data Breaches. McLaren knew that the sensitive personal data with which it was entrusted would be a lucrative target for hackers.

88. Despite such knowledge, McLaren failed to implement and maintain reasonable and appropriate data privacy and security measures to protect Plaintiffs' and Class Members' Private Information from cyber-attacks that McLaren should have anticipated and guarded against.

89. Data breaches, including those perpetrated against healthcare entities that store Private Information in their systems, have become widespread.

90. In the third quarter of the 2023 fiscal year alone, 733 organizations experienced data breaches, resulting in 66,658,764 individuals' personal information

being compromised.[32]

91. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including HCA Healthcare (11 million patients, July 2023), Managed Care of North America (8 million patients, March 2023), PharMerica Corporation (5 million patients, March 2023), HealthEC LLC (4 million patients, July 2023), ESO Solutions, Inc. (2.7 million patients, September 2023), and Prospect Medical Holdings, Inc. (1.3 million patients, July-August 2023), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

92. Cybercriminals seek out PHI at a greater rate than other sources of personal information. In a 2023 report, the healthcare compliance company Protenus found there were 956 medical data breaches in 2022 with over 59 million patient records exposed. This is an increase from the 758 medical data breaches which exposed approximately 40 million records that Protenus compiled in 2020.

93. Defendant knew and understood that unprotected or exposed Private Information in the custody of healthcare entities, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Private Information through unauthorized access.

---

[32] *See* https://www.idtheftcenter.org/post/q3-2023-data-breach-report-itrc-reports-data-compromise-record-with-three-months-left-in-year/ (last accessed Oct. 17, 2024).

94. At all relevant times, McLaren knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

95. Indeed, cyber-attacks, such as the two experienced by McLaren here, have become so notorious that the Federal Bureau of Investigation and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[33]

96. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

97. The injuries to Plaintiffs and Class Members were directly and

[33] Kochman, Ben, *FBI, Secret Service Warn Of Targeted Ransomware*, LAW360, (Nov. 18, 2019), https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection.

proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

98. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiffs and Class Members are long lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years.

99. As a healthcare entity in custody of current and former patients' and other affiliated persons' Private Information, Defendant knew, or should have known, the importance of safeguarding Private Information entrusted to it by Plaintiffs and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breaches.

Value of Private Information

100. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[34] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security

[34] 17 C.F.R. § 248.201 (2013).

number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[35]

101. PII and PHI are valuable property rights. Their value as a commodity is measurable. "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[36] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018. It is so valuable to identity thieves that once Private Information has been disclosed, criminals often trade it on the cyber black market or the dark web, for many years.

102. The PHI/PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[37]

103. As a result of the real and significant value of this material, identity thieves and other cyber criminals have openly posted credit card numbers, Social

---

[35] *Id.*

[36] OECD, *Exploring the Economics of Personal Data*, *A Survey of Methodologies for Measuring Monetary Value*, (Apr. 2, 2013) https://www.oecd-ilibrary.org/exploring-the-economics-of-personal-data_5k486qtxldmq.pdf.

[37] George, Anita, *Your personal data is for sale on the dark web. Here's how much it costs*, DIGITAL TRENDS, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.

Security numbers, Private Information, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breaches, can be readily aggregated, becoming more valuable to thieves and more damaging to victims.

104. For example, PII can be sold at a price ranging from $40 to $200.[38] Bad actors can purchase access to entire company data breaches from $900 to $4,500.[39]

105. PII can sell for as much as $363 per record according to the Infosec Institute.[40] PII is particularly valuable because criminals can use it to target victims with frauds and scams.

106. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

107. PHI is particularly valuable and has been referred to as a "treasure trove for criminals" – a cybercriminal who steals a person's PHI can end up with as many

---

[38] Stack, Brian, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN, (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web.

[39] *In the Dark*, VPNOverview, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Oct. 17, 2024).

[40] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

as "seven to ten personal identifying characteristics of an individual."[41]

108. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[42]

109. According to account monitoring company LogDog, medical data sells for $50 and up on the Dark Web.[43]

110. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[44]

111. Among other forms of fraud, identity thieves may obtain driver's

---

[41] Steger, Andrew, *What Happens to Stolen Healthcare Data?*, HEALTHTECH, (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon.
[42] *See Medical I.D. Theft,* EFRAUDPROTECTION.NET, https://efraudprevention.net/home/education/?a=187 (last accessed Sept. 24, 2024).
[43] Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, NAKED SECURITY (Oct. 3, 2019), https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content.
[44] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD, (Feb. 6, 2015), https://www. networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

licenses, government benefits, medical services, and housing or even give false information to police.

112. The fraudulent activity resulting from the Data Breaches may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[45]

McLaren Fails to Comply With FTC Guidelines

113. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

114. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal patient

[45] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[46]

115. The guidelines also recommend that healthcare businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[47]

116. The FTC further recommends that healthcare companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

117. The FTC has brought enforcement actions against healthcare entities for failing to protect patient data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access

[46] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[47] *Id.*

to confidential patient data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

118. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g.*, *In the Matter of LabMd, Inc., A Corp*, 2016-2 Trade Cas. (McLaren) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

119. Defendant failed to properly implement basic data security practices.

120. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

121. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the Private Information of its patients, and it was also aware of the significant repercussions that would result from its failure to do so.

McLaren Fails to Comply With HIPAA Guidelines

122. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R.

Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

123. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[48] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

124. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

125. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred electronically.

126. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

127. "Electronic protected health information" is "individually identifiable health information . . . that is (i) transmitted by electronic media; maintained in

[48] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

electronic media." 45 C.F.R. § 160.103.

128. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

129. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Defendant is also required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

130. HIPAA and HITECH also obligate Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

131. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of a data breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[49]

132. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

133. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

134. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and

[49] *Breach Notification Rule*, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added) (last accessed Oct. 17, 2024).

appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule."[50] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says "represent the industry standard for good business practices with respect to standards for securing e-PHI."[51]

McLaren Fails to Comply With Industry Standards

135. As noted above, experts studying cyber security routinely identify healthcare entities in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which healthcare entities collect and maintain.

136. Several best practices have been identified that, at a minimum, should be implemented by healthcare entities in possession of Private Information, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication;

[50] US Department of Health & Human Services, *Security Rule Guidance Material*, http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last accessed Oct. 17, 2024).
[51] US Department of Health & Human Services, *Guidance on Risk Analysis*, https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last accessed Oct. 17, 2024).

backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

137. Other best cybersecurity practices that are standard in the healthcare industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train its staff.

138. On information and belief, Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

139. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and upon information and belief, Defendant failed to comply with at least one – or all – of these accepted standards, thereby

opening the door to the threat actor and causing the Data Breaches.

Common Injuries and Damages

140. Theft of Private Information is serious. The FTC warns consumers that identity thieves use Private Information to exhaust financial accounts, receive medical treatment, start new utility accounts, and incur charges and credit in a person's name.

141. As a result of Defendant's ineffective and inadequate data security practices, the resulting two Data Breaches, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiffs and Class Members has materialized and is imminent, and Plaintiffs and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their Private Information; and (e) the continued risk to their Private Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' Private Information.

The Data Breaches Increase Victims' Risk of Identity Theft

142. Plaintiffs and Class Members are at a heightened risk of identity theft

for years to come. Identity thieves use personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. Experian, one of the largest credit reporting companies in the world, warns consumers that identity thieves can profit off your personal information by, among other things, selling the information, taking over accounts, using accounts without permission, applying for new accounts, obtaining medical procedures, filing a tax return, and applying for government benefits.

143. Plaintiffs' counsel have confirmed that the unencrypted Private Information of Class Members has already been posted for sale on the dark web by the cybercriminal group, BlackCat. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the Private Information of Plaintiffs and Class Members.

144. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize the information. Criminals monetize the data by selling the stolen information on the black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

145. Because a person's identity is akin to a puzzle with multiple data points,

the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to further track the victim and obtain additional data to more easily perpetrate a crime.

146. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. A data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data breaches can be the starting point for these additional targeted attacks on the victim.

147. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[52]

[52] "Fullz" describes data that includes the information of the victim, including, but not limited to, the name, address, credit card information, Social Security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), available at https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-

148. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

149. The development of "Fullz" packages means that the stolen Private Information from the Data Breaches here can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breaches, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

150. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the Data Breaches can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and Class Members.

151. Theft of Social Security numbers also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of their Social Security number, and a new Social Security number will not be

---

stolen-from-texas-life-insurance-firm (last accessed Oct. 17, 2024).

provided until after the harm has already been suffered by the victim.

152. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other Private Information (e.g., names, addresses, and dates of birth) is akin to having a master key to the gates of fraudulent activity. Data security researcher Tom Stickley, hired by companies to find flaws in their computer systems, has stated, "If I have your name and your Social Security number and you don't have a credit freeze yet, you're easy pickings."[53] Then, this comprehensive dossier can be sold—and then resold in perpetuity—to bad actors (i.e., scam telemarketers).

153. Theft of Private Information is even more serious when it includes theft of PHI. Data breaches involving medical information "typically leave[] a trail of falsified information in medical records that can plague victims' medical and financial lives for years."[54] It "is also more difficult to detect, taking almost twice as long as normal identity theft."[55] In warning consumers on the dangers of medical identity theft, the FTC states that an identity thief may use Private Information "to

[53] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say,* TIME (August 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security.
[54] World Privacy Forum, *Medical Identity Theft*, https://www.worldprivacyforum.org/category/med-id-theft (last accessed Oct. 17, 2024).
[55] FBI Cyber Division, *Health Care Systems and Medical Devices at Risk for Increased Cyber Intrusions for Financial Gain*, (Apr. 7, 2014), https://info.publicintelligence.net/FBI-HealthCareCyberIntrusions.pdf.

see a doctor, get prescription drugs, buy medical devices, submit claims with your insurance provider, or get other medical care."[56] The FTC also warns, "If the thief's health information is mixed with yours it could affect the medical care you're able to get or the health insurance benefits you're able to use."[57]

154. A report published by the World Privacy Forum and presented at the US FTC Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected.
- Significant bills for medical goods and services neither sought nor received.
- Issues with insurance, co-pays, and insurance caps.
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime. For example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed due to medical activities of the imposter; and victims have been denied jobs due to incorrect information placed in their health files due to the crime.
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts.

[56] FTC, *What To Know About Medical Identity Theft*, (May 2021), https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft.
[57] *Id.*

- Phantom medical debt collection based on medical billing or other identity information.

- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[58]

155. There may also be a time lag between when sensitive personal information is stolen, when it is illicitly used, and when a person discovers the illicit usage. For example, it takes approximately three months on average for consumers to discover that their identity has been stolen and used, but it takes some individuals up to three years to learn that information.

156. It is within this context that Plaintiffs and Class Members must now live with the knowledge that their Private Information is forever in cyberspace and was taken by and in the possession of people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

Loss of Time to Mitigate Risk of Identity Theft and Fraud

157. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified that their Private Information has been compromised, as in these Data Breaches, a reasonable person is expected to take

[58] Dixon, Pam & Emerson, John, *The Geography of Medical Identity Theft*, WORLD PRIVACY FORUM, (Dec. 12, 2017), https://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf).

steps and time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft or fraud. Failure to spend time taking steps to review accounts or credit reports could expose an individual to greater financial harm – ultimately, the resource and asset of time has been lost.

158. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must monitor their financial accounts for many years to mitigate the risk of identity theft.

159. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as monitoring their accounts for fraudulent activity and checking their credit reports for unusual activity.

160. Plaintiffs' and Class Members' mitigation efforts, including those who experience actual identity theft and fraud, are consistent with the U.S. Government Accountability Office's 2007 report regarding data breaches, the GAO Report, in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[59]

161. Plaintiffs' mitigation efforts are also consistent with the steps that the

[59] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/new.items/d07737.pdf.

FTC recommends data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (if someone steals their identity, an extended fraud alert that lasts for seven years is suggested), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[60]

Diminution of Value of Private Information

162. PII and PHI are valuable property rights.[61] Their value is axiomatic, considering the value of an individual's data in today's economy and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

163. A robust legitimate marketplace for Private Information exists. In 2019, the data brokering industry was worth roughly $200 billion.[62]

---

[60] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last accessed Sept. 24, 2024).

[61] *See, e.g.*, Randall T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[62] *See* Lazarus, David, *Shadowy data brokers make the most of their invisibility cloak*, LOS ANGELES TIMES (Nov. 5, 2019) https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

164. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[63,64]

165. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[65]

166. As a result of the Data Breaches, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

167. Thus, the information compromised in the two Data Breaches is significantly more valuable than the loss of, for example, payment card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. Upon information and belief, the information compromised in these Data Breaches is impossible to "close" and difficult, if not impossible, to change.

---

[63] *See, e.g.*, https://datacoup.com/ (last accessed Oct. 17, 2024).
[64] *See, e.g.*, https://digi.me/how (last accessed Oct. 17, 2024).
[65] Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last accessed Sept. 24, 2024).

168. The fraudulent activity resulting from the Data Breaches may not come to light for years.

169. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

170. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to the detailed Private Information of, upon information and belief, 2.5 million individuals, and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

171. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiffs and Class Members.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

172. Given the type of targeted attack in this case and related sophisticated criminal activity, the type of Private Information involved, and the volume of data obtained in the Data Breaches, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web

for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes (e.g., opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; take out loans or lines of credit; or file false unemployment claims).

173. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her personal information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

174. Consequently, Plaintiffs and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

175. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft that arose from Defendant's Data Breaches.

Loss of the Benefit of the Bargain

176. Furthermore, McLaren's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. When agreeing to pay Defendant and/or its agents for the provision of medical services, directly or indirectly, Plaintiffs and other reasonable consumers understood and expected that they were,

in part, paying for the service and necessary data security to protect the Private Information, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

PLAINTIFFS' EXPERIENCES

Plaintiff Drugich

177. Plaintiff Cheryl Drugich is a current patient at McLaren.

178. In order to obtain medical services at McLaren, she was required to provide it with her PII and PHI.

179. Upon information and belief, at the time of the Data Breaches, Defendant retained Plaintiff Drugich's Private Information in its system.

180. Plaintiff Drugich is very careful about sharing her sensitive Private Information. Plaintiff Drugich stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Drugich would not have entrusted her Private Information to Defendant had she known of Defendant's inadequate data security policies.

181. Plaintiff Drugich received a Notice Letter from Defendant, informing her that her PII and/or PHI was improperly accessed and obtained by unauthorized

third parties in connection with the 2023 Data Breach. Upon information and belief, and based upon a good faith investigation conducted by Plaintiffs' counsel, some or all of the same PII and PHI that Plaintiff Drugich entrusted to McLaren was also compromised in the 2024 Data Breach.

182. As a result of the Data Breaches, Plaintiff Drugich made reasonable efforts to mitigate the impact of the Data Breaches, including monitoring her accounts for fraudulent activity and checking her credit reports for unusual activity. Plaintiff Drugich has spent significant time dealing with the Data Breaches—valuable time Plaintiff Drugich otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

183. Plaintiff Drugich suffered actual injury from having her Private Information compromised as a result of the Data Breaches including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; and (vii) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains

backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

184. The Data Breaches have caused Plaintiff Drugich to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the respective Data Breaches' occurrence.

185. As a result of the Data Breaches, Plaintiff Drugich anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breaches.

186. As a result of the Data Breaches, Plaintiff Drugich is at a present and continued increased risk of identity theft and fraud for years to come.

187. Plaintiff Drugich has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Norwood

188. Plaintiff Janise Norwood is a past and current patient at McLaren.

189. In order to obtain medical services at McLaren, she was required to provide it with her PII and PHI.

190. Upon information and belief, at the time of the Data Breaches, Defendant retained Plaintiff Norwood's Private Information in its system.

191. Plaintiff Norwood is very careful about sharing her sensitive Private Information. Plaintiff Norwood stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Norwood would not have entrusted her Private Information to Defendant had she known of Defendant's inadequate data security policies.

192. Plaintiff Norwood received a Notice Letter from Defendant, informing her that her PII and/or PHI was improperly accessed and obtained by unauthorized third parties in connection with the 2023 Data Breach. Upon information and belief, and based upon a good faith investigation conducted by Plaintiffs' counsel, some or all of the same PII and PHI that Plaintiff Norwood entrusted to McLaren was also compromised in the 2024 Data Breach.

193. As a result of the Data Breaches, Plaintiff Norwood made reasonable efforts to mitigate the impact of the Data Breaches, including replacing impacted debit cards. Plaintiff Norwood has spent significant time dealing with the Data Breaches—valuable time Plaintiff Norwood otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

194. Plaintiff Norwood suffered actual injury from having her Private Information compromised as a result of the Data Breaches including, but not limited

to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; and (vii) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

195. Plaintiff Norwood also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breaches.

196. The Data Breaches have caused Plaintiff Norwood to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the respective Data Breaches' occurrence.

197. As a result of the Data Breaches, Plaintiff Norwood anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breaches.

198. As a result of the Data Breaches, Plaintiff Norwood is at a present and

continued increased risk of identity theft and fraud for years to come.

199. Plaintiff Norwood has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Porter

200. Plaintiff Melissa Porter is a current patient at McLaren.

201. In order to obtain medical services at McLaren, she was required to provide it with her PII and PHI.

202. Upon information and belief, at the time of the Data Breaches, Defendant retained Plaintiff Porter's Private Information in its system.

203. Plaintiff Porter is very careful about sharing her sensitive Private Information. Plaintiff Porter stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Porter would not have entrusted her Private Information to Defendant had she known of Defendant's inadequate data security policies.

204. Plaintiff Porter received a Notice Letter from Defendant, informing her that her PII and/or PHI was improperly accessed and obtained by unauthorized third parties in connection with the 2023 Data Breach. Upon information and belief, and based upon a good faith investigation conducted by Plaintiffs' counsel, some or all

of the same PII and PHI that Plaintiff Porter entrusted to McLaren was also compromised in the 2024 Data Breach.

205. As a result of the Data Breaches, Plaintiff Porter made reasonable efforts to mitigate the impact of the Data Breaches, including monitoring her accounts for fraudulent activity, closing financial accounts, and contacting Defendant to obtain more details about the Data Breaches. Plaintiff Porter has spent significant time dealing with the Data Breaches—valuable time Plaintiff Porter otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

206. Plaintiff Porter suffered actual injury from having her Private Information compromised as a result of the Data Breaches including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; and (vii) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate

measures to protect the Private Information.

207. Plaintiff Porter additionally suffered actual injury in the form of a credit account being falsely opened under her name, according to Experian and Credit Karma, which, upon information and belief, was caused by the Data Breaches.

208. Plaintiff Porter further suffered actual injury in the form of experiencing fraudulent charges to her Free Star Financial Credit Union Account, in or about September 2023 and December 2023, which, upon information and belief, was caused by the Data Breaches.

209. Plaintiff Porter also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breaches.

210. In addition, Plaintiff Porter suffered injury in the form of being charged for medical services from a facility of Defendant's for services that she did not seek or receive, which, upon information and belief, was caused by the Data Breaches.

211. Moreover, Plaintiff Porter experienced actual injury in the form of her Private Information being disseminated on the dark web, according to Experian and Credit Karma, which, upon information and belief, was caused by the Data Breaches.

212. The Data Breaches have caused Plaintiff Porter to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the respective Data Breaches' occurrence. Plaintiff

Porter has increased her prescribed medication for anxiety as a result of the Data Breach.

213. As a result of the Data Breaches, Plaintiff Porter anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breaches.

214. As a result of the Data Breaches, Plaintiff Porter is at a present and continued increased risk of identity theft and fraud for years to come.

215. Plaintiff Porter has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff McSkulin

216. Plaintiff Jamie McSkulin is a current patient at McLaren.

217. In order to obtain medical services at McLaren, she was required to provide it with her PII and PHI.

218. Upon information and belief, at the time of the Data Breaches, Defendant retained Plaintiff McSkulin's Private Information in its system.

219. Plaintiff McSkulin is very careful about sharing her sensitive Private Information. Plaintiff McSkulin stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured

source. Plaintiff McSkulin would not have entrusted her Private Information to Defendant had she known of Defendant's inadequate data security policies.

220. Plaintiff McSkulin received a Notice Letter from Defendant, informing her that her PII and/or PHI was improperly accessed and obtained by unauthorized third parties in connection with the 2023 Data Breach. Upon information and belief, and based upon a good faith investigation conducted by Plaintiffs' counsel, some or all of the same PII and PHI that Plaintiff McSkulin entrusted to McLaren was also compromised in the 2024 Data Breach.

221. As a result of the Data Breaches, Plaintiff McSkulin made reasonable efforts to mitigate the impact of the Data Breaches, including replacing impacted debit cards. Plaintiff McSkulin has spent significant time dealing with the Data Breaches—valuable time Plaintiff McSkulin otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

222. Plaintiff McSkulin suffered actual injury from having her Private Information compromised as a result of the Data Breaches including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to

mitigate the actual consequences of the Data Breaches; and (vii) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

223. Plaintiff McSkulin further suffered actual injury in the form of experiencing fraudulent charges to her Team One Credit Union debit card, for approximately $150, which, upon information and belief, was caused by the Data Breaches.

224. Plaintiff McSkulin also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breaches.

225. The Data Breaches have caused Plaintiff McSkulin to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the respective Data Breaches' occurrence. Plaintiff McSkulin is especially fearful of identity theft, which she reports thinking like it could happen at *any* time in the future.

226. As a result of the Data Breaches, Plaintiff McSkulin anticipates spending considerable time and money on an ongoing basis to try to mitigate and

address harms caused by the Data Breaches.

227. As a result of the Data Breaches, Plaintiff McSkulin is at a present and continued increased risk of identity theft and fraud for years to come.

228. Plaintiff McSkulin has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Wells

229. Plaintiff Tamyra Ejuan Wells is a current patient at McLaren.

230. In order to obtain medical services at McLaren, she was required to provide it with her PII and PHI.

231. Upon information and belief, at the time of the Data Breaches, Defendant retained Plaintiff Wells's Private Information in its system.

232. Plaintiff Wells is very careful about sharing her sensitive Private Information. Plaintiff Wells stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Wells would not have entrusted her Private Information to Defendant had she known of Defendant's inadequate data security policies.

233. Upon information and belief, Plaintiff Wells's PII and/or PHI was improperly accessed and obtained by unauthorized third parties in the Data

Breaches.

234. As a result of the Data Breaches, Plaintiff Wells made reasonable efforts to mitigate the impact of the Data Breaches, including monitoring her accounts for fraudulent activity, researching the Data Breaches, and changing passwords. Plaintiff Wells has spent significant time dealing with the Data Breaches—valuable time Plaintiff Wells otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

235. Plaintiff Wells suffered actual injury from having her Private Information compromised as a result of the Data Breaches including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; and (vii) the continued and certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

236. Plaintiff Wells also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breaches.

237. The Data Breaches have caused Plaintiff Wells to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the respective Data Breaches' occurrence.

238. As a result of the Data Breaches, Plaintiff Wells anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breaches.

239. As a result of the Data Breaches, Plaintiff Wells is at a present and continued increased risk of identity theft and fraud for years to come.

240. Plaintiff Wells has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Beasley

241. Plaintiff Ashley Beasley is a former patient at McLaren.

242. In order to obtain medical services at McLaren, she was required to provide it with her PII and PHI.

243. Upon information and belief, at the time of the Data Breaches, Defendant retained Plaintiff Beasley's Private Information in its system.

244. Plaintiff Beasley is very careful about sharing her sensitive Private Information. Plaintiff Beasley stores any documents containing Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Beasley would not have entrusted Private Information to Defendant had she known of Defendant's inadequate data security policies.

245. Plaintiff Beasley received a Notice Letter from Defendant, informing her that her PII and/or PHI was improperly accessed and obtained by unauthorized third parties in in connection with the 2023 Data Breach. Upon information and belief, and based upon a good faith investigation conducted by Plaintiffs' counsel, some or all of the same PII and PHI that Plaintiff Beasley entrusted to McLaren was also compromised in the 2024 Data Breach.

246. As a result of the Data Breaches, Plaintiff Beasley made reasonable efforts to mitigate the impact of the Data Breaches, including monitoring her accounts for fraudulent activity, changing passwords, and contacting banks regarding fraudulent activity. Plaintiff Beasley has spent significant time dealing with the Data Breaches–valuable time Plaintiff Beasley otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

247. Plaintiff Beasley suffered actual injury from having her Private

Information compromised as a result of the Data Breaches including, but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

248. Plaintiff Beasley additionally suffered actual injury in the form of two attempts to open credit cards falsely under her name at Capital One and Citi Bank, which, upon information and belief, was caused by the Data Breaches.

249. Plaintiff Beasley further suffered actual injury in the form of experiencing a fraudulent attempt to agree to be bound by a lease under her name by a caller in Atlanta, Georgia who sought to obtained a copy of her mortgage company so that it could be sent to a leasing company, which, upon information and belief, was caused by the Data Breaches, and which has caused her to expend time and effort in contesting and mitigating the impact of this attempted fraud, and which,

additionally, has caused Plaintiff Beasley stress and anxiety.

250. Plaintiff Beasley also suffered actual injury in the form of experiencing suspicious activity to her Equifax account, forcing her to place a security freeze and fraud alert on her account. Upon information and belief, this suspicious activity was caused by the Data Breaches.

251. Plaintiff Beasley also suffered actual injury in the form of hard inquiries and other suspicious activity on her Experian account, forcing her to place a security freeze on her personal credit report. Upon information and belief, these hard inquiries and suspicious activity was caused by the Data Breaches.

252. Plaintiff Beasley also suffered actual injury in the form of experiencing suspicious activity on her TransUnion credit file, forcing her to place a fraud alert and security freeze on her file. Upon information and belief, this suspicious activity was caused by the Data Breaches.

253. In addition, Plaintiff Beasley suffered injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breaches.

254. Moreover, Plaintiff Beasley experienced actual injury in the form of her Private Information being disseminated on the dark web, which, upon information and belief, was caused by the Data Breaches.

255. The Data Breaches have caused Plaintiff Beasley to suffer fear, anxiety,

and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the respective Data Breaches' occurrence. Plaintiff Beasley's increased anxiety has caused her to lose sleep, as a result of the Data Breaches.

256. As a result of the Data Breaches, Plaintiff Beasley anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breaches.

257. As a result of the Data Breaches, Plaintiff Beasley is at a present and continued increased risk of identity theft and fraud for years to come.

258. Plaintiff Beasley has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Turri

259. Plaintiff Kyle Turri is a former patient at Defendant.

260. In order to obtain medical services at McLaren, he was required to provide it with his PII and PHI.

261. Upon information and belief, at the time of the Data Breaches, Defendant retained Plaintiff Turri's Private Information in its system.

262. Plaintiff Turri is very careful about sharing his sensitive Private Information. Plaintiff Turri stores any documents containing his Private Information

in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Turri would not have entrusted his Private Information to Defendant had he known of Defendant's inadequate data security policies.

263. Plaintiff Turri received a Notice Letter from Defendant, informing him that his PII and/or PHI was improperly accessed and obtained by unauthorized third parties in connection with the 2023 Data Breach. Upon information and belief, and based upon a good faith investigation conducted by Plaintiffs' counsel, some or all of the same PII and PHI that Plaintiff Turri entrusted to McLaren was also compromised in the 2024 Data Breach.

264. As a result of the Data Breaches, Plaintiff Turri made reasonable efforts to mitigate the impact of the Data Breaches, including contacting Coinbase, filing a police report, researching the Data Breaches, filing a FTC identity theft report, contacting credit bureaus to place freezes on his accounts, and going to banks to place alerts on his accounts. Plaintiff Turri has spent significant time dealing with the Data Breaches–valuable time Plaintiff Turri otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

265. Plaintiff Turri suffered actual injury from having his Private Information compromised as a result of the Data Breaches including, but not limited

to: (i) invasion of privacy; (ii) theft of his Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; and (vii) the continued and certainly increased risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

266. Plaintiff Turri further suffered actual injury in the form of experiencing a fraudulent account being opened under his name and then the debit card being used to withdraw approximately $9,000 from his Coinbase account in or about August 2023. Upon information and belief, this unauthorized transaction was caused by the Data Breaches.

267. Plaintiff Turri also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breaches.

268. The Data Breaches have caused Plaintiff Turri to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully

informed him of key details about the respective Data Breaches' occurrence.

269. As a result of the Data Breaches, Plaintiff Turri anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breaches.

270. As a result of the Data Breaches, Plaintiff Turri is at a present and continued increased risk of identity theft and fraud for years to come.

271. Plaintiff Turri has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Stebbins

272. Plaintiff Trista Wynn Stebbins is a current patient at Defendant.

273. In order to obtain medical services at Defendant, she was required to provide her Private Information to Defendant.

274. Upon information and belief, at the time of the Data Breaches, Defendant retained Plaintiff Stebbins' Private Information in its system.

275. Plaintiff Stebbins is very careful about sharing her sensitive Private Information. Plaintiff Stebbins stores any documents containing her Private Information in a safe and secure location. She has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Stebbins would not have entrusted her Private Information to

Defendant had she known of Defendant's inadequate data security policies.

276. Plaintiff Stebbins received a Notice Letter from Defendant, informing her that her PII and/or PHI was improperly accessed and obtained by unauthorized third parties in connection with the 2023 Data Breach. Upon information and belief, and based upon a good faith investigation conducted by Plaintiffs' counsel, some or all of the same PII and PHI that Plaintiff Stebbins entrusted to McLaren was also compromised in the 2024 Data Breach.

277. As a result of the Data Breaches, Plaintiff Stebbins made reasonable efforts to mitigate the impact of the Data Breaches, including contacting Defendant. Plaintiff Stebbins has spent significant time dealing with the Data Breaches—valuable time Plaintiff Stebbins otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

278. Plaintiff Stebbins suffered actual injury from having her Private Information compromised as a result of the Data Breaches including, but not limited to: (i) invasion of privacy; (ii) theft of her Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; and (vii) the continued and

certainly increased risk to her Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

279. Plaintiff Stebbins also suffered actual injury in the form of experiencing an increase in spam calls, texts, and/or emails, which, upon information and belief, was caused by the Data Breaches.

280. The Data Breaches have caused Plaintiff Stebbins to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the respective Data Breaches' occurrence.

281. As a result of the Data Breaches, Plaintiff Stebbins anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breaches.

282. As a result of the Data Breaches, Plaintiff Stebbins is at a present and continued increased risk of identity theft and fraud for years to come.

283. Plaintiff Stebbins has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ACTION ALLEGATIONS

284. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

285. Specifically, Plaintiffs propose the following class definitions, subject to amendment as appropriate:

> **Nationwide Class**
> All persons in the United States whose PII and/or PHI was compromised as a result of one or both of the Data Breaches (the "Nationwide Class").
>
> **Michigan Subclass**
> All persons in the state of Michigan whose PII and/or PHI was compromised as a result of one or both of the Data Breaches (the "Michigan Subclass").

286. Excluded from the Classes are Defendant and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

287. Plaintiffs reserve the right to modify or amend the definition of the proposed Classes, as well as add subclasses, before the Court determines whether certification is appropriate.

288. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

289. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Although the precise number of such persons is currently unknown to Plaintiffs and exclusively in the possession of McLaren, according to the Michigan Attorney General and *Data Breach Today*, at least 2.5 million persons were impacted in the Data Breaches.[66] Thus, the Class is sufficiently numerous to warrant certification.

290. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant's conduct violated the FTCA and/or HIPAA;

c. When Defendant learned of the respective Data Breaches;

d. Whether Defendant's response to each of the Data Breaches was adequate;

e. Whether Defendant unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

f. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breaches;

g. Whether Defendant's data security systems prior to and during the Data Breaches complied with applicable data security laws and regulations;

[66] *McGee*, *supra*, n.13.

h. Whether Defendant's data security systems prior to and during the Data Breaches were consistent with industry standards;

i. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

j. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the Data Breaches;

l. Whether Defendant had a legal duty to provide timely and accurate notice of the Data Breaches to Plaintiffs and Class Members;

m. Whether Defendant breached its duty to provide timely and accurate notice of the Data Breaches to Plaintiffs and Class Members;

n. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiffs and Class Members suffered as a result of Defendant's misconduct;

p. Whether Defendant's conduct was negligent;

q. Whether Defendant was unjustly enriched;

r. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;

s. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

291. Typicality. Plaintiffs' claims are typical of those of other Class

Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breaches. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendant. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

292. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

293. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

294. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find the cost of litigating their individual claims to be prohibitively high and would thus have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

295. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Defendant has acted and/or refused to act on grounds generally applicable to Class Members such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

296. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to the names and addresses and/or email addresses of Class Members affected by the Data Breaches.

CAUSES OF ACTION

COUNT I

Negligence

(On Behalf of Plaintiffs and the Nationwide Class and Michigan Subclass)

297. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

298. Defendant requires its patients, including Plaintiffs and Class Members, to submit non-public PII and PHI in the ordinary course of providing its medical services.

299. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of its business of soliciting its services to its patients, which solicitations and services affect commerce.

300. Plaintiffs and Class Members entrusted Defendant with their Private Information and understood that Defendant would safeguard their information.

301. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed. It also was specifically warned about the potential of an attack by BlackCat.

302. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendant had a reasonable duty of care to use reasonable means to secure and safeguard their computer systems—and Class Members' Private Information held within it—to prevent

disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach. Additionally, Defendant's duty is based on the requirements of MCL 500.1406 as a healthcare corporation operating in the State of Michigan.

303. Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

304. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

305. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements

discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

306. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its patients. That special relationship arose because Plaintiffs and Class Members entrusted Defendant with their confidential Private Information, a necessary part of being patients of Defendant. Moreover, Defendant was in an exclusive position to know the extent of its data security capabilities and to detect and prevent the Data Breaches.

307. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

308. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or Class Members.

309. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former patients' Private Information that it was no longer required to retain pursuant to regulations.

310. Moreover, Defendant had a duty to promptly and adequately notify Plaintiffs and Class Members of the Data Breaches.

311. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

312. Defendant breached its duties, pursuant to the FTC Act, HIPAA, and other applicable standards, and thus were negligent, by failing to use reasonable measures to protect Class Members' Private Information. Defendant's specific negligent acts and omissions include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

f. Failing to remove former patients' Private Information that it was no longer required to retain pursuant to regulations; and

g. Failing to timely and adequately notify Class Members about the Data Breaches' respective occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other

damages.

313. Defendant violated Section 5 of the FTC Act and HPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and Class Members.

314. Plaintiffs and Class Members are within the class of persons that the FTC Act and HIPAA were intended to protect.

315. The harm that occurred as a result of the Data Breaches is the type of harm the FTC Act and HIPAA were intended to guard against.

316. Defendant's violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

317. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

318. A breach of security, unauthorized access, and resulting injury to Plaintiffs and Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

319. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breaches of security were reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare industry.

320. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information were wrongfully disclosed.

321. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the Private Information of Plaintiffs and Class Members, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on Defendant's systems.

322. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

323. Plaintiffs and Class Members had no ability to protect their Private Information that was in, and possibly remains in, Defendant's possession.

324. Defendant was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breaches.

325. Defendant's duty extended to protecting Plaintiffs and Class Members from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

326. Defendant has admitted that the Private Information of Plaintiffs and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breaches.

327. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the Private Information of Plaintiffs and Class Members would not have been compromised.

328. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and Class Members and the harm, or risk of imminent harm, suffered by Plaintiffs and Class Members. The Private Information of Plaintiffs and Class Members was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

329. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

330. As a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

331. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant

fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

332. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breaches.

333. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and insecure manner.

334. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class and Michigan Subclass)

335. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

336. Plaintiffs and Class Members were required to provide their Private Information to Defendant as a condition of receiving medical services from Defendant.

337. Plaintiffs and Class Members entrusted their Private Information to

Defendant. Defendant accepted Plaintiffs' and Class Members' personal medical information for the purpose of providing services for Plaintiffs and Class Members, thereby entering an implied contract whereby Defendant became obligated to reasonably safeguard Plaintiffs' and Class Members' personal medical information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached and compromised or stolen.

338. Implicit in the agreement between Defendant and Plaintiffs and Class Members to provide Private Information, was Defendant's obligation to: (a) use such Private Information for business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent unauthorized disclosures of the Private Information, (d) provide Plaintiffs and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their Private Information, (e) reasonably safeguard and protect the Private Information of Plaintiffs and Class Members from unauthorized disclosure or uses, and (f) retain the Private Information only under conditions that kept such information secure and confidential.

339. The mutual understanding and intent of Plaintiffs and Class Members on the one hand, and Defendant, on the other, is demonstrated by their conduct and course of dealing.

340. Defendant solicited, offered, and invited Plaintiffs and Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiffs and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

341. In accepting the Private Information of Plaintiffs and Class Members, Defendant understood and agreed that it was required to reasonably safeguard the Private Information from unauthorized access or disclosure.

342. On information and belief, at all relevant times Defendant promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiffs and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breaches.

343. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' Private Information would remain protected.

344. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

345. Plaintiffs and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

346. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

347. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of Defendant's implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

348. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

349. Defendant breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their Private Information, and by failing to timely delete certain Private Information, and by failing to provide accurate notice that Private Information was compromised as a result of the Data Breaches.

350. As a direct and proximate result of Defendant's breach of the implied contracts, Plaintiffs and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

351. Plaintiffs and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breaches.

352. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring

procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT III
Breach of Express Contract
(On Behalf of Plaintiffs and the Nationwide Class and Michigan Subclass)

353. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

354. As discussed above, Defendant affirmatively agreed to protect the security of the PII and PHI provided to it by its patients. These express representations appeared in McLaren's Compliance Program and Resources page, its Standards of Conduct, its Notice of Privacy Protection, and its Privacy Policy.

355. Defendant's data security promises were a material term of Plaintiffs' and Class Members' agreement to utilize a McLaren hospital for medical services.

356. Defendant breached its express contractual obligations to reasonably protect and secure the PII and PHI of Plaintiffs and Class Members.

357. Defendant's breach caused damages to Plaintiffs and Class Members, including nominal damages.

COUNT IV
Violation of the Michigan Consumer Protection Act
(MCL § 445.901, *et seq.*)
(On Behalf of Plaintiffs and the Michigan Subclass)

358. Plaintiffs repeat and re-allege each and every factual allegation

contained in all previous paragraphs as if fully set forth herein and brings this count on behalf of themselves and the Michigan Subclass.

359. Plaintiffs are authorized to bring this claim under MCL § 445.911.

360. The Michigan Consumer Protection Act ("MCPA"), MCL § 445.901, *et seq.*, prohibits "unfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce[.]" MCL § 445.903(1).

361. As described herein, Defendant has engaged in the following unfair, unconscionable, and deceptive trade practices that are made unlawful under the MCPA, MCL § 445.903(1):

> (c) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has sponsorship, approval, status, affiliation, or connection that she or she does not have;
>
> (e) Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or mode, if they are of another;
>
> (s) Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer; and
>
> (cc) Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner.

362. Defendant made affirmative representations, including "pledges" and "commitments" to protect the security of Plaintiffs' and Michigan Subclass Members' Private Information, but Defendant failed to implement measures to protect Plaintiffs' and Michigan Subclass Members' Private Information, failed to

respond to affirmative warnings of security threats from the specific threat actors that executed the Data Breaches, failed to identify foreseeable security risks and vulnerabilities in its network, failed to take reasonable steps to mitigate and defend against the threat posed by the threat actor, and failed to notify Plaintiffs and Michigan Subclass Members of the Data Breaches in a timely manner.

363. Defendant omitted and actively concealed material facts regarding its inadequate security policies and practices from Plaintiffs and the Michigan Subclass and withheld and continues to withhold information regarding the nature and extent of the Data Breaches. Had Defendant disclosed that its data systems lacked the almost universal safeguards described above, or had it disclosed that it had been warned of the likelihood that it would be targeted by a ransomware attack and refused or neglected to take the mitigating and defensive measures the state of Michigan had recommended, Plaintiffs and Michigan Subclass Members would not have allowed Defendant to collect and maintain their Private Information.

364. Defendant's deceptive acts or practices in the conduct of commerce include, but are not limited to:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Michigan Subclass Members' Private Information, which was a direct and proximate cause of the Data Breaches;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents in the

industry, which were direct and proximate causes of the Data Breaches;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' Private Information, including but not limited to duties imposed by the FTC Act, which were direct and proximate causes of the Data Breaches;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs; and Michigan Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiffs' and Michigan Subclass Members' Private Information;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Michigan Subclass Members' Private Information;

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law, statutory, and self-imposed duties pertaining to the security and privacy of Plaintiffs' and Michigan Subclass Members' Private Information; and

h. Failing to promptly and adequately notify Plaintiffs and Michigan Subclass Members that their Private Information was accessed by unauthorized persons in the Data Breaches.

365. Defendant is engaged in, and its acts and omissions affect, trade and commerce. Defendant's relevant acts, practices, and omissions complained of in this action were done in the course of Defendant's business of marketing, offering for sale, and selling goods and services throughout the United States.

366. Defendant had exclusive knowledge of material information regarding its deficient security policies and practices, and regarding the security of Plaintiffs'

and Class Members' Private Information. This exclusive knowledge includes, but is not limited to, information that Defendant received through internal and other non-public audits and reviews that concluded that Defendant's security policies were substandard and deficient, and that Plaintiffs' and Michigan Subclass Members' Private Information and other Defendant data was vulnerable.

367. Defendant had exclusive knowledge about the extent of the Data Breaches, including during the days, weeks, and months following the Data Breaches.

368. Defendant also had exclusive knowledge about the length of time that it maintained individuals' Private Information after they stopped using services that necessitated the transfer of that Private Information to Defendant.

369. Defendant failed to disclose, and actively concealed, the material information it had regarding Defendant's deficient security policies and practices, and regarding the security of the sensitive PII and PHI. For example, even though Defendant has long known, through internal audits and otherwise, that its security policies and practices were substandard and deficient, and that Plaintiffs' and Michigan Subclass Members' Private Information was vulnerable as a result, Defendant failed to disclose this information to, and actively concealed this information from, Plaintiffs, Michigan Subclass Members, and the public. Defendant also did not disclose, and actively concealed, information regarding the

extensive length of time that it maintains former patients' and other affiliated persons' Private Information and other records. Likewise, during the days and weeks following the Data Breaches, Defendant failed to disclose, and actively concealed, information that it had regarding the extent and nature of the Data Breaches.

370. Defendant had a duty to disclose the material information that it had because, *inter alia*, it had exclusive knowledge of the information, it actively concealed the information, and because Defendant was in a fiduciary position by virtue of the fact that Defendant collected and maintained Plaintiffs' and Michigan Subclass Members' PII and PHI.

371. Defendant's representations and omissions were material because they were likely to deceive reasonable individuals about the adequacy of Defendant's data security and its ability to protect the confidentiality of current and former patients' and other affiliated persons' Private Information.

372. Had Defendant disclosed to Plaintiffs and Michigan Subclass Members that its data systems were not secure and, thus, vulnerable to attack, Defendant would have been unable to continue in business without adopting reasonable data security measures and complying with the law. Instead, Defendant received, maintained, and compiled Plaintiffs' and Michigan Subclass Members' Private Information without advising that Defendant's data security practices were insufficient to maintain the safety and confidentiality of their Private Information.

373. Accordingly, Plaintiffs and Michigan Subclass Members acted reasonably in relying on Defendant's misrepresentations and omissions, the truth of which they could not have discovered.

374. Defendant's practices were also contrary to legislatively declared and public policies that seek to protect data and ensure that entities who solicit or are entrusted with personal data utilize appropriate security measures, as reflected in laws, such as HIPAA and the FTC Act.

375. Defendant generated revenue by way of Plaintiffs and Michigan Subclass Members paying or generating medical insurance payments when entering transactions with Defendant where Defendant was the direct beneficiaries of these payments. Defendant's services were of lesser value than Defendant represented in that Defendant did not take reasonable measures to safeguard patients/consumers' personal medical information. In reliance on Defendant's misrepresentations about its products and services, Plaintiffs and Michigan Subclass Members entered transactions with Defendant that they would not have, or for which Plaintiffs and Michigan Subclass Members would have paid less but for Defendant's representations.

376. The injuries suffered by Plaintiffs and Michigan Subclass Members greatly outweigh any potential countervailing benefit to patients/consumers or to competition and are not injuries that Plaintiffs and Michigan Subclass Members

should have reasonably avoided.

377. The damages, ascertainable losses and injuries, including to their money or property, suffered by Plaintiffs and Michigan Subclass Members as a direct result of Defendant's deceptive acts and practices as set forth herein include, without limitation: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

378. Plaintiffs and Michigan Subclass Members seek all monetary and non-monetary relief allowed by law, including actual or nominal damages; declaratory and injunctive relief, including an injunction barring Defendant from disclosing their Private Information without their consent; reasonable attorneys' fees and costs; and any other relief that is just and proper.

COUNT V
Violation of the Michigan Data Breach Notification Statute
(MCL § 445.73(13))
(On Behalf of Plaintiffs and the Michigan Subclass)

379. Plaintiffs repeat and re-alleges each and every factual allegation contained in all previous paragraphs as if fully set forth herein and brings this count on behalf of themselves and the Michigan Subclass.

380. Plaintiffs are authorized to bring this claim under MCL § 445.73(13).

381. Defendant is a corporation that owns, maintains, and records PII and PHI, and computerized data including PII and PHI, about its current and former patients and other affiliated persons, including Plaintiffs and Michigan Subclass Members.

382. Defendant is in possession of PII and PHI belonging to Plaintiffs and Michigan Subclass Members and is responsible for reasonably safeguarding that PII and PHI consistent with the requirements of MCL § 445.72.

383. Defendant failed to safeguard, maintain, and dispose of, as required, the PII within its possession, custody, or control as discussed herein, which it was required to do by Michigan law.

384. Defendant, knowing and/or reasonably believing that Plaintiffs' and Michigan Subclass Members' PII and PHI was acquired by unauthorized persons during the Data Breaches, failed to provide reasonable and timely notice of the Data Breaches to Plaintiffs and Michigan Subclass Members, as required by MCL §

445.72(1), (4). Indeed, as of the date of the filing of this First Amended Complaint, McLaren has not provided any individual notice whatsoever with respect to the 2024 Data Breach.

385. As a result of Defendant's failure to reasonably safeguard Plaintiffs' and Michigan Subclass Members' Private Information, and the failure to provide reasonable and timely notice of the Data Breaches to Plaintiffs and Michigan Subclass Members, Plaintiffs and Michigan Subclass Members have been damaged as described herein, continue to suffer injuries as detailed above, are subject to the continued risk of exposure of their Private Information in Defendant's possession, and are entitled to damages in an amount to be proven at trial.

COUNT VI
Violation of the Nonprofit Health Care Corporation Reform Act
(MCL 500.1406)
(On Behalf of Plaintiffs and the Michigan Subclass)

386. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

387. At all relevant times, Defendant was a "healthcare corporation" under the terms of MCL 500.1406 as an entity organized under sections 501(a) and 501(c) of the IRS Code and as a "nonprofit hospital service corporation," "medical care corporation," or a "consolidated hospital service," as defined by Michigan law.

388. At all relevant times, Plaintiffs and Michigan Subclass Members were "members" under the terms of MCL 500.1406 as subscribers, the dependents of

subscribers, or other individuals entitled to receive health care benefits under a nongroup or group certificate under Michigan law.

389. By the acts described above, Defendant violated MCL 500.1406 by collecting, maintaining, and controlling its patients' sensitive personal medical information in a negligent and reckless manner and by designing, maintaining, and controlling systems that exposed its patients' sensitive personal medical information of which Defendant had control and possession to the risk of exposure to unauthorized persons, thereby violating its duty to implement and maintain reasonable security procedures and practices appropriate to protect the Private Information given the nature of this information. Defendant allowed unauthorized users to view, use, manipulate, exfiltrate, and steal the nonencrypted and nonredacted Private Information of Plaintiffs and Michigan Subclass Members, including their personal medical information.

390. As a result of Defendant's violations, Plaintiffs and Michigan Subclass Members are entitled to all actual and compensatory damages according to proof or statutory damages allowable under MCL 500.1406, whichever are higher, to reasonable attorneys' fees and costs, and to such other and further relief as this Court may deem just and proper.

COUNT VII
Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class and Michigan Subclass)

391. Plaintiffs repeat and re-allege each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

392. This count is pleaded in the alternative to Plaintiffs' breach of implied and express contract claims above (Count II and Count III).

393. Plaintiffs and Class Members conferred a monetary benefit on Defendant. Specifically, they paid for services from Defendant and/or its agents and in so doing also provided Defendant with their Private Information. In exchange, Plaintiffs and Class Members should have received from Defendant the services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

394. Defendant knew that Plaintiffs and Class Members conferred a benefit on it in the form of their Private Information as well as payments made by them or on their behalf as a necessary part of their receiving healthcare services. Defendant accepted and realized that benefit. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

395. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiffs and Class Members.

396. As such, a portion of the payments made for the benefit of or on behalf of Plaintiffs and Class Members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

397. Defendant, however, diverted funds intended to be applied towards data security to its own profit and failed to adequately fund its data security program sufficient to secure Plaintiffs' and Class Members' Private Information from unauthorized access and, therefore, did not provide adequate data security in return for the benefit Plaintiffs and Class Members provided.

398. Defendant would not be able to carry out an essential function of its regular business without the Private Information of Plaintiffs and Class Members and derived revenue by using it for business purposes. Plaintiffs and Class Members expected that Defendant or anyone in Defendant's position would use a portion of that revenue to fund adequate data security practices.

399. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

400. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have allowed their Private Information to be provided to Defendant.

401. Defendant enriched itself by saving the costs it reasonably should have

expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Instead of providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profit at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures and diverting those funds to its own profit. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and the safety of their Private Information.

402. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money wrongfully obtained from Plaintiffs and Class Members because Defendant failed to implement appropriate data management and security measures that are mandated by industry standards.

403. Plaintiffs and Class Members have no adequate remedy at law.

404. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches; and (vii) the continued and

certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

405. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

406. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that Defendant unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendant's services.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Nationwide Class and Michigan Subclass;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

C. For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to patient data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the two Data Breaches;

D. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. Prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. Requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. Requiring Defendant to delete, destroy, and purge the Private Information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. Requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the Private Information of Plaintiffs and Class Members;

v. Prohibiting Defendant from maintaining the Private Information of Plaintiffs and Class Members on a cloud-based database;

vi. Requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. Requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. Requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. Requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. Requiring Defendant to conduct regular database scanning and securing checks;

xi. Requiring Defendant to establish an information security training program that includes at least annual information security training for all patients, with additional training to be provided as appropriate based upon the patients' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. Requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. Requiring Defendant to implement a system of tests to assess its respective patients' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing patients' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. Requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. Requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves; and

xvi. Requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and

xvii. Appointing a qualified and independent third party assessor, for a period of ten years, to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Class, and to report any deficiencies with compliance of the Court's final judgment.

E. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

F. Ordering Defendant to pay for not less than ten years of credit monitoring services for Plaintiffs and Class Members;

G. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

H. For an award of punitive damages, as allowable by law;

I. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

J. Pre- and post-judgment interest on any amounts awarded; and

K. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Dated: October 17, 2024 Respectfully submitted,

/s/ E. Powell Miller
E. Powell Miller (P39487)
Emily E. Hughes (P68724)

THE MILLER LAW FIRM
950 W. University Drive, Suite 300
Rochester, MI 48307
T: (248) 841-2200
epm@millerlawpc.com
eeh@millerlawpc.com

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
T: (866) 252-0878
gklinger@milberg.com

Benjamin F. Johns
Samantha E. Holbrook
SHUB & JOHNS LLC
Four Tower Bridge
200 Barr Harbor Drive, Suite 400
Conshohocken, PA 19428
T: (610) 477-8380
bjohns@shublawyers.com
sholbrook@shublawyers.com

Interim Co-Lead Counsel

Andrew W. Ferich
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
T: (310) 474-9111
aferich@ahdootwolfson.com

Nick Suciu
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN LLC
6905 Telegraph Rd., Suite 115
Bloomfield Hills, MI 48301

Tel: (313) 303-3472
Email: nsuciu@milberg.com

Bryan L. Bleichner (MN BAR #0326689)
Philip J. Krzeski (OH BAR #0095713)
CHESTNUT CAMBRONNE PA
100 Washington Ave South, Ste 1700
Minneapolis, MN 55401
T: (612) 339-7300
bbleichner@chestnutcambronne.com
pkrzeski@chestnutcambronne.com

Terry R. Coates (OH BAR #0085579)
MARKOVITS STOCK & DEMARCO, LLC
119 E. Court Street, Ste 530
Cincinnati, OH 45202
T: (513) 651-3700
tcoates@msdlegal.com

Jeff Ostrow
Ken Grunfeld
KOPELOWITZ OSTROW, P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
T: (954) 525-4100
ostrow@kolawyers.com
grunfeld@kolawyers.com

Julie Erickson, SBN 293111
(julie@eko.law)
Elizabeth Kramer, SBN 293129
(elizabeth@eko.law)
Kevin Osborne, SBN 261367
(kevin@eko.law)
ERICKSON KRAMER OSBORNE LLP
44 Tehama Street
San Francisco, CA 94105
T: (415) 635-0631

James J. Pizzirusso
HAUSFELD LLP
888 16th Street N.W.
Suite 300
Washington, D.C. 20006
T: (202) 540-7200
Email: jpizzirusso@hausfeld.com

Steven M. Nathan
HAUSFELD LLP
33 Whitehall Street
Suite 1400
New York, NY 10004
T: (646) 357-1100
Email: snathan@hausfeld.com

Robert C. Schubert
Amber L. Schubert
SCHUBERT JONCKHEER & KOLBE LLP
2001 Union St, Ste 200
San Francisco, CA 94123
T: (415) 788-4220
rschubert@sjk.law
aschubert@sjk.law

Rod M. Johnston (P80337)
JOHNSTON LAW, PLLC
6911 Duchess Court
Troy, MI 48098
T: (586) 321-8466
rod@johnstonlawflsa.com

Additional Counsel for Plaintiffs and the Putative Class

CERTIFICATE OF SERVICE

I hereby certify that on October 17, 2024, I electronically filed the foregoing document(s) using the Court's electronic filing system, which will notify all counsel of record authorized to receive such filings.

/s/ E. Powell Miller
E. Powell Miller (P39487)
THE MILLER LAW FIRM, P.C.
950 W. University Dr., Ste. 300
Rochester, MI 48307
Tel: (248) 841-2200
epm@millerlawpc.com